UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT
EASTERN DIVISION OF OHIO

In the Matter of the Search of:	)	**No.** 2:21-mj-365
	)	
The premises located at 1266 Olde Henderson Square, Columbus, OH including curtilage or detached buildings/garages, and any computers or related digital media, or digital devices located therein; the person of Kenneth Ogudu, and any computers or digital media located thereon.	)	**Magistrate Judge**
		UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Terry Hedrick, a Special Agent with the United States Secret Service (USSS) being first duly sworn, hereby depose and state as follows:

AFFIANT'S BACKGROUND AND EXPERIENCE

1. I am a Special Agent with the United States Secret Service (hereinafter, the "USSS"), Charleston, WV Resident Office, and have been so employed since December of 2004. I am authorized, pursuant to 18 U.S.C. § 3056(b), to detect and arrest any person who violates any of the laws of the United States relating to electronic fund transfer frauds, access device frauds, false identification documents or devices, and any fraud or criminal or unlawful activity or against any federally insured financial institution. Additionally, I am authorized, pursuant to 18 U.S.C. § 3056(c), to execute warrants issued under the laws of the United States.

2. Since becoming a Secret Service Special Agent, I have personally investigated and/or assisted in investigations relating to violations of the laws of the United States relating to financial crimes, including romance frauds and other online schemes, specifically 18 U.S.C. § 1341 (mail fraud), 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. §§ 1956-57 (money laundering) and

18 US.C. 2315 (receipt of stolen property). I received 30 weeks of training at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia, and Secret Service's Rowley Training Center in Beltsville, Maryland, before my assignment as a Secret Service Special Agent in the Charleston, WV Resident Office. Several of these investigations have resulted in criminal prosecutions in the United States District Court in the Southern District of West Virginia.

3. As a Special Agent with the USSS, I have been involved in other financial elder abuse and romance fraud investigations. I know from my training and experience that those persons involved in committing those types of crimes spend a great deal of time each week seeking out potential victims through email, text messages, social media websites such as Google Hangouts, Go Fish, Plenty of Fish and various dating sites. I also know that people who commit these crimes stay in constant contact with victims, creating a friendship that ultimately leads to a false romantic relationship with victims. I know that these fraudsters tell their victims untrue stories about their employment, their personal life, their family life and their need for financial assistance. In many of these instances, the fraudsters propose marriage to the victim. I know that after this romance flourishes, the fraudsters then ask victims to send them money for various reasons. Some of the fraudsters' reasons include family medical emergencies, or because the fraudsters need to pay their oil rig workers, or need money to ship gold or other valuables back to the United States to be allegedly shared with the victims or finally, for bail when the fraudsters were allegedly arrested after leaving a foreign country.

4. I know from my training and experience that these fraudsters instruct their victims to send large amounts of currency through the U.S. Mail, FedEx and through the United Parcel Service (UPS). I know that these fraudsters get their victims to send money to them via cashier checks, personal checks, money orders, wire transfers, bitcoin and through many different mobile

payment processing companies. These mobile payment processing companies include Transferwise, Ping Express, Money Gram, Western Union, Walmart, Pay Pal, Square, Cash App, Xoom, Zelle, and others.

5. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents, investigators and witnesses. This Affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information contained in this Affidavit is taken from financial records, interviews with witnesses, and information shared with me from other investigators and state officials. This ongoing investigation is financial in nature, thus, any figures I cite in this Affidavit are based on calculations and tracing conducted to date and may be subject to revision at a later date.

6. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1341, 1343, 1956-57 and 2315 have been committed by Kenneth EMENI ("EMENI"), John NASSY ("NASSY"), Kenneth OGUDU also known as Kenneth Lee ("OGUDU"), Oluwagbenga HARRISON ("HARRISON"), Oluwabanishe AWOLESI also known as Oluwabamishe Johnson ("AWOLESI"), Romello Thorpe ("THORPE") (collectively, the "Targets").

7. I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 1341 (mail fraud); 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1344 (bank fraud); 18 U.S.C. § 1956 (laundering in monetary transactions in property derived from specified unlawful activity); 18 U.S.C. § 1957 (engaging in monetary transactions in property derived from specified unlawful activity) and 18 U.S.C. 2315 (receipt of stolen property), and I am authorized by law to request a search warrant.

PURPOSE OF THIS AFFIDAVIT

8. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in Attachment A of this Affidavit, including those properties and/or persons listed below (collectively the "SUBJECT PREMISES") for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1341 (mail fraud); 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1956 (laundering in monetary transactions in property derived from specified unlawful activity); 18 U.S.C. § 1957 (engaging in monetary transactions in property derived from specified unlawful activity); and 18 U.S.C. § 2315 (Receipt of Stolen Property), which items are more specifically described in Attachment B of this Affidavit. This Affidavit is also being submitted in support of an application under Rule 41 of the Federal Rules Criminal Procedure for a search warrant for the SUBJECT PREMISES in order to effectuate the arrests of EMENI, NASSY, OGUDU, HARRISON, AWOLESI, and THORPE.

a. OGUDU

i. The person of OGUDU

ii. The entire property located 1266 Olde Henderson Square, Columbus, OH 43220, including mailboxes, trash containers, debris boxes, located therein;

1. 1266 Olde Henderson Square, Columbus, OH 43220 is believed to be OGUDU's current residence. Investigators have learned this information from surveillance and records obtained during the investigation. Pursuant to a conversation with OGUDU's landlord, investigators

learned that OGUDU moved to the SUBJECT PREMISES in February 2020 and is scheduled to be evicted from the SUBJECT PREMISES on May 31, 2021. In addition, on May 11, 2021, investigators obtained a warrant for geolocation data associated with OGUDU's cellphone. A review of this data shows that OGUDU is still presently residing at the SUBJECT PREMISES. On or about May 16, 2021, investigators conducted in-person surveillance of the SUBJECT PREMISES and noted that a vehicle[1] registered to OGUDU was parked outside of the SUBJECT PREMISES address as well.

2. OGUDU resided at the SUBJECT PREMISES during a portion of the fraud scheme, specifically, he lived there during the interactions with Victim L.T.

iii. the content of computers and electronic storage devices located and seized therein; and

iv. the content of any locked cabinets, containers, drawers, boxes or other receptacles large enough for paper record retention or electronic storage devices located therein.

9. This Affidavit is also submitted in support of an application for a search warrant for the person described in Attachment A of this Affidavit, OGUDU. As set forth herein, there is

[1] This Affiant is not requesting to search the vehicle but noting its presence as another factor demonstrating that OGUDU still resides at 1266 Olde Henderson Square at this time.

probable cause to search the person of OGUDU, as described in Attachment A, for the items described in Attachment B, including cell phones and digital storage devices such as thumb drives that can be concealed on their person should OGUDU be present in the SUBJECT PREMISES. I believe probable cause exists for the issuance of a warrant to search OGUDU as described in Attachment A, for (1) property that constitutes evidence of a federal criminal offense; (2) contraband, the fruits of a federal crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means for committing a federal criminal offense, namely 18 U.S.C. § 1341 (mail fraud); 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1956 (laundering in monetary transactions in property derived from specified unlawful activity); 18 U.S.C. § 1957 (engaging in monetary transactions in property derived from specified unlawful activity); and 18 U.S.C. § 2315 (receipt of stolen property).

10. From my background and experience, I know that individuals normally maintain records of their financial activity, such as receipts for expenditures by cash and check, bank records, tax returns, escrow files, and other financial documents, in their personal residences and places of business. I am also aware that individuals engaged in illegal activity often possess computers, documents, storage devices, and electronic media used in the commission of the crime and, as set forth below, the Targets have been known to use computers and other electronic devices.

11. There are many reasons why individuals, including criminal offenders, maintain evidence for long periods of time. The evidence may be necessary business records which must be kept for information reporting purposes, such as for state and Federal tax returns, and loan applications. The evidence may also appear innocuous at first glance (e.g., financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets,

personal calendars, telephone and address directories, check books, videotapes and photographs of vacations or other residences, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone bills, keys to safe deposit boxes, packaging materials, computer hardware and software), but may have real significance and relevance when considered in light of other evidence. The individual or business entity at issue may no longer realize they still possess the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The individual may also be under the mistaken belief that they have deleted, hidden, or further destroyed any computer-related evidence, but which may actually be retrievable by a trained forensic computer expert as detailed later in this Affidavit.

12. Through my training and experience, I am aware that the proceeds generated from both legal and illegal activities may be spent many years after the illegal activity has ceased. Thus, records reflecting income and expenditures for the time period spanning the scheme and associated activity and those years immediately following the end of such activity are also essential to any financial investigation.

13. The statements in this Affidavit are based in part on information provided by other investigators, state and local law enforcement officers, witnesses, records obtained through investigation, as well as straining and experience and my own investigation of this matter. This ongoing investigation is financial in nature, thus, any figures I cite in this Affidavit are based on calculations and tracing conducted to date and may be subject to revision at a later date. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations or attempted violations of 18 U.S.C. § 1341

(mail fraud); 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1956 (laundering in monetary transactions in property derived from specified unlawful activity); 18 U.S.C. § 1957 (engaging in monetary transactions in property derived from specified unlawful activity); and 18 U.S.C. § 2315 are presently located in the SUBJECT PREMISES.

STATUTORY AUTHORITY

14. As noted above, this investigation concerns alleged violations of the following:

a. **18 U.S.C. § 1341** prohibits the use of the postal service or commercial interstate carrier to carry out a scheme to defraud.

b. **18 U.S.C. § 1343** prohibits the use of wire, radio, or television communication in interstate or foreign commerce to carry out a scheme to defraud.

c. **18 U.S.C. § 1956** prohibits conducting a financial transaction with proceeds from a specified unlawful activity to promote the unlawful activity or conceal its proceeds.

d. **18 U.S.C. § 1957** prohibits money transactions involving criminally derived proceeds of a value greater than $10,000.

e. **18 U.S.C. § 2315** prohibits the sale or receipt of stolen goods or money more than $5,000 that has crossed interstate lines.

DEFINITIONS

15. The following definitions apply to this Affidavit and Attachment B:

a. "**Online schemes**" targeted persons looking for romantic partners, friendship, and other close personal and business relationships on dating websites and other social media platforms. The perpetrators of the schemes, also referred to as "fraudsters or scammers within this Affidavit," created profiles using

fictitious and fake names, locations, images, and personas, allowing the perpetrators of the schemes to cultivate relationships with prospective victims. The victims provided money and gifts to the perpetrators of the schemes and were typically asked to conduct transactions on behalf of the perpetrators of the scheme.

b. "**Cryptocurrency**" was a form of non-fiat based digital currency, in which transactions are verified and records maintained by a decentralized system using computer data and codes, rather than by a centralized authority. Bitcoin was a type of cryptocurrency.

c. "**Shell Company**" refers to a purported business entity incorporated under state law that does not engage in any substantial legitimate business activity, but was instead used to perpetrate bank fraud, wire fraud, money laundering or other criminal offenses.

d. "**Financial institution**," as defined in 18 U.S.C. § 20, is an insured depository institution or credit union with accounts insured by the National Credit Union Share Insurance Fund.

e. The **Federal Deposit Insurance Corporation** ("**FDIC**") is an independent agency of the United States government that protects loss of insured monetary deposits if an FDIC-insured bank or savings association fails.

f. **Branch Banking & Trust ("BB&T")** now known as **"Truist," JP Morgan Chase, N.A. ("Chase"), TD AmeriTrade, Fifth Third Bank, Huntington National Bank, Bank of America, PNC Bank, SunTrust Bank ("SunTrust")** also now known as **"Truist,"** and **City National Bank** were

financial institutions of the Federal Deposit Insurance Act, within the meaning of 18 U.S.C. § 20.

g. **BB&T, Chase, TD AmeriTrade, Fifth Third Bank, Huntington National Bank, Bank of America, PNC Bank, SunTrust, and City National Bank** were financial institutions which engaged in, and the activities of which affected, interstate commerce as defined in 31 U.S.C. § 5312(a)(2).

h. **"Zelle"** was a digital payment network and part of a private financial services company owned by Bank of America, BB&T, Capital One, Chase, PNC Bank, U.S. Bank and Wells Fargo. Zelle allowed an individual to electronically transfer money from his or her bank account to another registered user's bank account, held within the United States, by using a mobile device or the website of a participating banking institution.

i. "**Computer**," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

j. "**Computer hardware**," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard

drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

k. "**Computer passwords**" and "**data security devices**," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, and reverse the process to restore it.

l. "**Mobile applications**," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, accessing banking information, and transferring monetary funds. Mobile applications are also referred to as "apps" throughout this Affidavit.

m. A "**Website**" consists of textual pages of information and associated graphic

images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

n. A "**storage medium**" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

o. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact disks, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE TO SEARCH THE PROPERTY DESCRIBED IN ATTACHMENT A AND TO SEIZE THE PROPERTY DESCRIBED IN ATTACHMENT B

16. In early 2016 through at least October 8, 2020, at or near Huntington, Cabell

County, West Virginia, within the Southern District of West Virginia, and elsewhere, the Targets and others worked together to carry out various online schemes and scams with victims, which caused the victims to send money to persons working with the defendants and to accounts controlled by the Targets. Specifically, the Targets and their associates would:

a. Target and contact victims via email, text messaging, or online dating websites and social media websites that fraudulently induced the victims into believing the victim was in a romantic relationship, friendship, or business relationship with a person using a false and fraudulent identity created by defendants and other members of the scheme;

b. Refuse to use FaceTime or any other video-chat technology with the victims in order to conceal their true identities;

c. Induce the victims to send money for a variety of false and fraudulent reasons to persons using fraudulent identities, when, in actuality, the accounts were controlled by defendants;

d. Direct victims to send payments via wire transfer services, including but not limited to bank wire, Western Union, and MoneyGram, to themselves or other individuals. At times, victims were directed to send payments to shell companies and accounts under defendants' control;

e. Direct victims to purchase cashier's checks and money orders which they then directed to identified parties and addresses using the United States Postal Service and other common couriers; and

f. Share the proceeds among themselves and with others through wire transfers, Zelle, Cash App and by cashing money orders and cashier's

checks.

17. The purpose of the fraud scheme was for defendants EMENI, NASSY, OGUDU, HARRISON, THORPE and AWOLESI to enrich themselves by falsely cultivating relationships through online scams with the victims and thereby causing the victims to send money to persons working with the defendants and to accounts controlled by defendants.

VICTIM[2] INFORMATION

18. Investigators interviewed over thirty individuals who transferred money to the Targets' bank accounts. Some of the information investigators learned from the victims and reviewing their financial records is described below. One similarity uniting all of the victims is that they transferred the money to the Targets upon the requests of the online fraudsters, even though the victims themselves did not know or ever communicate with men they knew to be EMENI, NASSY, OGUDU, HARRISON, AWOLESI or THORPE.

19. Investigators believe that the following individuals are victims of the fraud scheme: Kathy Bartley, Wain Beard, William Buerckholtz, Michael Cantrell, Ronald Compton, Equity Enterprises Inc., Thao Hong Hoang, Jill Hubbard, Thomas P. Jancsy, Lucinda Kendrick, Ashok Kumar, Rebbecca Levesque, Xinai Li, Baaki Abdul Majeed, Krolicki Mateusz, Sven Leo Ortloff, Alexsandra Palada, James C. Paul, Robert and Judith Pederson, Paula Qualls, Gerry Lee Wilwant, Daniel Worton, Ma Cecilia Yuson, Kent John Ramesh Abrahansson, Luisa Aguilar-Facun, Daniel Akogun, Mohammed Alghamdi, Roger Amick,James Amick, Podesta D. Anto, Karam Assad, Ahma Angelina Atchison, Diane Avino, Maria Rosa Garcia Barcellos, Kathyrn

[2] Investigators currently believe that the individuals labeled as victims in the next section and listed in Paragraph 19 are fraud victims. However, investigators may change their classification of these individuals if they learn more information which shows that one of the victims is more appropriately classified as a conspirator or a money mule.

Bautisa, Sondra Benson, Sue Belcher, Lim Heng Boon, Karen Botfield, Ruth Ann Brassfield, Chonticha Butchai, Carrie Calhoun, Olga Carasso, Patricia Carter, Martha Alicia Canedo Casique, Jana Celigova, Gina Champion, Onepark Rue Chaptal, Brenda Checci, Kalala Naomi Cherrelle, Romella Christain, Doris Clouser, Rose Coey, Linda M Collier, Maria Correia, Marvelle Crigger, Gayle Cunningham, Carla Monica Da Cunha, Thi Kim Hien Dang, Dianne Davis, Deborah K. Dawson, Kathie A. Day, Beverly Demmith, Clifton O. Dodge, Linda Dolstad, Naomi Draper, Jose Tuset Duran, Douglas Durbin, Ruth Eaton, Payam Ebrahimian, Embassy of the Argentine Republic, Elaine Elizabeth Ensor, Cathy Erdmann, Robert Fitzgerald, John P. Fleenor, Elaine Beverly Foli, Nicole Fuchshuber, Annita Gadola, Cristina Garcia, Selia Salazar Garcia, Jacklyn D. Giles, Teresa Graves, Laura Elizabeth Gricius, Alberto Gutierrez, Nazia Hafiz, Diana Hall, Linda Haran, Elizabeth Hart, Tuahe Hingano, Yen B. Ho, Nguyet Ho, Thao Hong Hoang, Connie Hoffman, Laura Holmes, Deborah L. Honeycutt, Ying Hong, Stacy Howell, Yi-Chun Huang, Imarie Hughes, Jenny Hughey, Hong X Huynh, Gladys Estela Garcia Jacquet, Connie Justice, Joshua J. Kanute, Akram Karimi, Jacquelyn Kelley, Roksana Khyznhiak, Soo Gyung Kim, Eddie Kirkland, Thipakron Kotmoongun, Emilia Krojerova, Moshe Lazorov, Catherine Le, Linda Leisner, Annie B. Lemons, Thelma Li Markham, Jill Sandra Liibus, Andre Lima, Chun Ting Liu, Gary J. Loar, Julie A. Loomis, Faye Loupe, Tatyana Lozinskaya, Pia Lundqvist, Mle Gwozdzik, Malgorata, Aaron T. Mancho, Angela Manzi, Gloria Marin, Penha Cristina Braga Martins, Cheryl A. Mazella, Linda Mills, Valentina Podbertcaia Chisinau Moldova, J Moral, Virginia Musgrave, Leonie Doreen Mairn, Valarie Nancy, Deborah Nedal, Thia Ngo, Long Hong Nguyen, Thanh Thi Diem Huynh Nguyen, Hoa V. Nguyen, Nancy Nguyen, Ernesto Javier Wright Tanca Nuria, S. E. Empey Ogb, Maria Lourdes Fevidal Opinion, Karl Owen, Nadezhda Panasyuk, Ama Maria De Torre Pancorbo, Jeffrey Paulus,Maribel Perez, Miriam L. Perez, Mai Pham, Tra My T Pham, Prem

Ka Ragupathy, Cathy Reed, Christiane Renken, Wanda Rhodes, Karen Robinson, Julie Stanford Rockett, Alejandra Saavedra, Intesta Sampaolo, Gloria Sandefur, Sandra L. Schwabenbauer, Celine Sergent, Alice Seymour, Hiba Sharaf, Francine Shokrany, Sherry Kay Stanley, D. G. Stern, Pearl Stilwell, Karen Sue Teamer, Cheryl Thomas, Abida Thompson, Krista L. Thompson, Erica Thumma, Pedro Cauhtemoc Torres, Jossie L. Torres, Cassandra Townsend, Maria Del Milagro Trevino, Cheng-Hsuan Tsai, Carii Uhl, Rmr Ik Umi, Esmeraldo Walker, Cynthia Ward, Maureen Elizabeth Warr, Renee Wautier, Cynthis Rae Williams, Joanne Woodward, Hsiao Ching Wu, Jiahang Wu, Yifan Yang, Janet Mary Young, Michelle Young, and Cynthia Zo.

20. On April 28, 2021, EMENI, NASSY, AMECHI, OGUDU, HARRISON, AWOLESI, and THORPE were indicted in the Southern District of West Virginia on various charges of wire fraud, mail fraud, money laundering, and receipt of stolen property. Their criminal case number is 3:21-cr-00068. The allegations in the Indictment stemmed from the Targets' interactions with many of the victims described below. The Indictment is still sealed and not known to the Targets.

Victim R.B.

21. Victim R.B. met a man on Instagram who she knew as Mason George ("Mason") around December 2018. Victim R.B. communicated daily with Mason via text messages and WhatsApp. Mason told Victim R.B. he worked on an Exxon Mobile oil rig in the Gulf of Mexico. Around December 2018, Mason told her his oil rig crew was running out of food and Victim R.B. sent a wire transfer at Mason's request.

22. Victim R.B. sent a wire transfer on August 28, 2019 for $9,000 to Kenneth OGUDU at Chase Bank in Huntington, WV. This document reflects the purpose of the wire transfer was "personal loan." Victim R.B. told investigators that Mason told her to tell her bank

that was the purpose of the wire transfer. Victim R.B. stated that Mason called her on this date and advised he was on his way to Louisiana to see her when he was kidnapped by drug dealers in New Orleans. Mason told Victim R.B. that the drug dealers gave him the phone so he could call her and get the ransom money. Mason asked Victim R.B. to wire $9,000 to Kenneth OGUDU for his ransom. Victim R.B. stated this purpose of the wire transfer on the form was false but she did as Mason requested. Victim R.B. never met or communicated with OGUDU.

23. Victim R.B. wired $3,000 to OGUDU's Chase Bank account on August 30, 2019. Victim R.B. also wired another $10,000 to OGUDU on September 9, 2019. These wire transfer documents reflect the purpose of the wire transfers was "personal loan." Victim R.B. stated that Mason called her again and advised her the kidnappers wanted more money. Mason told her to wire another $3,000.00 to OGUDU for the ransom. Victim R.B. admitted the stated purpose of the wire transfer on the bank form was false but she did as Mason directed.

24. Victim R.B. sent a wire transfer on September 9, 2019, for $10,000 to EMENI at City National Bank in West Virginia from her account at Mid-South Bank. This document reflects the purpose of the wire transfer was for a "personal loan." Victim R.B. stated that Mason called her again on this date and advised her the kidnappers wanted even more money. Mason told her to send another $10,000 to EMENI to pay the ransom. Victim R.B. stated this purpose of the wire transfer on the bank form was false but that Mason told her to tell her bank that was the purpose of the wire transfer. Victim R.B. never met or communicated with Kenneth EMENI.

25. Victim R.B. stated that Mason called her and advised he had been kidnapped by drug dealers again on his way to see her in Louisiana. Mason told her a man named Benjamin was going to come to her house to get the ransom money. When Benjamin never showed up Mason called Victim R.B. again and asked Victim R.B. to wire $12,000 for the ransom to one of

the Targets' associates, Augustine Amechi. On February 21, 2020, Victim R.B. wired Augustine Amechi $12,000 even though she never met or communicated with him.

Example of Victim R.B. Wire Transfer to OGUDU

International ☐ Domestic ☑
Fee $60.00 – Cutoff Time: 2:00 pm Fee $25.00 – Cutoff Time 3:00 pm
Purpose of Wire: Personal Loan

MidSouth Bank

Outgoing Transfer Form

Email wires not permitted; Phone/Fax wires not permitted over $5,000,000.00
Signed wire agreements required for wire transfers greater than $100,000 via Phone & Fax.

Originator Information:

$ 10,000.00	Ruth Ann Brassfield
Amount of Wire – (Funds must be available)	Contact Person 254-631-9357
[redacted] Account #	Contact #
Ruth Ann Brassfield	NA
Title of Account	Email Address

Wire to (Crediting Bank Information):

021000021	Chase
ABA # (9 digits), OR SWIFT Code, OR BIC, OR IBAN, OR Account #	Bank Name
1000 5th Ave	Huntington, WV 25701
Address	City, State, Zip / City and Country

For Credit Of (Beneficiary-who is the wire benefitting-Bank or Individual):

503285907	Kenneth Ogudu
ABA # (9digits), OR SWIFT Code, OR BIC, OR IBAN, OR Account #	Bank Name or Individual's Name
2457 30th St	Huntington, WV 25703
Address of Beneficiary	City, State, Zip / City & Country of Beneficiary

For Further Credit Of (Final Beneficiary-If Applicable):

Account #	Beneficiary Name
Address	City, State, Zip / City & Country of Beneficiary

Memo:

In Person Wire Requests:
I hereby authorize MidSouth Bank to process an outgoing wire transfer on my behalf as instructed on this form. I understand the amount of the wire and any applicable fees will be debited from the account listed above. The information provided is true and correct to the best of my knowledge. I understand the receiving bank indicated on this form may apply the funds based on the account number alone, whether correct or incorrect, and I agree that MidSouth Bank is not held liable if the funds are not received by the receiving bank or beneficiary due to incorrect or incomplete instructions.

Customer Signature: Ruth Brassfield

Customer Information must be verified.

Fax & Phone Wire Requests:
☐ Phone (Domestic Only) ☐ $100,000+ passcode provided
☐ Form Faxed
☐ Agreement in Synergy ☐ Agreement Attached
Spoke to:

I verify that I spoke to the person listed above confirming the wire information.

Verification Completed by whom:

(employee signature)

Victim F.L.

26. Victim F.L. started communicating with a man who introduced himself as James Morrison, ("Morrison") online in early 2019. Morrison contacted her several times a week initially, and then communicated with her sometimes several times a day and a romance developed. Morrison told Victim F.L. he owned a construction company in Ohio, but that he was taking a construction job in Turkey. He told Victim F.L. that he could not use his credit card in Turkey and thus, could not pay his hotel bills and living expenses.

27. Victim F.L. stated she sent money at Morrison's direction on several occasions, but never sent money directly to Morrison. Victim F.L. believes she sent three or four wire transfers to others at Morrison's direction. On July 9, 2019, Victim F.L. sent a $50,000 Cashier's check, made payable to Kenneth OGUDU, that she purchased from her bank, the Louisiana Federal Credit Union at Morrison's direction. Morrison told Victim F.L. to put OGUDU as the payee and she mailed this check to OGUDU in Huntington, WV. She does not know or ever met OGUDU. Morrison told Victim F.L. that OGUDU would get these funds to him. Bank records reveal that OGUDU deposited this $50,000 Cashier's check into his bank account and did not make a subsequent $50,000 transfer to another individual.

Victim H.H.

28. Victim H.H. sent the following wire transfers from her bank in Pennsylvania to EMENI, HARRISON, NASSY and OGUDU in Huntington, West Virginia:

Date	Amount	Recipient	Stated Purpose
April 15, 2019	$6,400	EMENI	Purchase of Equipment
April 18, 2019	$4,700	HARRISON	Purchase of Equipment
May 1, 2019	$8,400	EMENI	Purchase of Equipment
May 9, 2019	$5,000	EMENI	Purchase of Equipment
May 13, 2019	$4,000	EMENI	Purchase of Equipment
May 20, 2019	$4,500	EMENI	Purchase of Equipment
May 28, 2019	$7,000	NASSY	Purchase of Equipment
August 28, 2019	$3,000	OGUDU	Purchase of Equipment
November 12, 2019	$6,000	OGUDU	Purchase of Equipment

December 19, 2019	$5,000	EMENI	Purchase of Equipment
December 20, 2019	$4,100	EMENI	Purchase of Equipment

29. During Victim H.H.'s interview, she stated that she was not a victim of fraud but sent these wires to order equipment for her restaurant. However, Victim H.H. could not remember what pieces of equipment she ordered with the wire transfers. Thus, Victim H.H. is classified as a victim for the purposes of this Affidavit, but the investigation may later reveal that she is a co-conspirator.

Victim J.H.

30. Victim J.H., who resides in Michigan, told investigators that she met a man, who identified himself as Daniel Moore ("Moore"), online in 2016. Moore told Victim J.H. he was a civil engineer and he was working on an oil rig in Dubai. About one month after meeting Moore, Moore started asking for money to pay his workers. Victim J.H. sent money at Moore's direction via Money Gram and wire transfers. She never sent the money directly to Moore, but always sent the money to other third-parties as Moore directed. Moore assured Victim J.H. that the recipients would forward the funds to him.

31. Victim J.H. stated that Moore allegedly died in December 2017. Shortly after learning of Moore's death, Victim J.H. was contacted by a female named "Ieasha," who also claimed to be from Dubai. Ieasha advised Victim J.H. that Moore's employer owed Moore a large amount of money (about $3,000,000) and that Moore listed Victim J.H. as his beneficiary. Ieasha told Victim J.H. she (Ieasha) would help Victim J.H. collect the money from Moore's estate. Before Victim J.H. could get these funds, she had to pay the Dubai government around $5,000.

32. Victim J.H. stated she sent the following amounts of money at Ieasha's direction. Victim J.H. never sent the funds directly to Ieasha, instead Ieasha instructed Victim J.H. to send

the money to the individuals listed below and then claimed these individuals would forward the money her. Victim J.H. never met or previously communicated with EMENI, HARRISON or THORPE but transferred funds to these individuals pursuant to Ieasha and Moore's instructions.

Date	Recipient	Amount	Method	Purpose
8/19/17	EMENI	$900	Western Union	Pay Moore's workers
12/14/17	HARRISON	$725	Money Gram	Pay Moore's workers
1/18/18	EMENI	$34,500	Wire transfer	Taxes for $3,000,000 she inherited from Moore per Ieasha
9/13/19	Thorpe	$35,000	Wire Transfer	Ieasha instructed Victim J.H. to tell the bank that the purpose of the transfer was for a quilting machine and Victim J.H. cannot recall the true purpose of the transfer

33. After Victim J.H. wired THORPE $35,000 on September 13, 2019, THORPE made three electronic payments to Kenneth OGUDU with these fraud proceeds. On September 19, 2019, he sent two separate payments to OGUDU, one for $2,000 and one for $5,000. On September 20, 2019, he made another payment of $7,000 to OGUDU.

34. Earlier, investigators received search warrants for various email accounts used by the identities that the victims communicated with and for the email addresses associated with the Targets. The investigation revealed that one of the email addresses associated with OGUDU is an email address martinun242@gmail.com. Examples of OGUDU using the martin242@gmail.com are shown below:

From: WorldRemit Support <customerservice@worldremit.com>
To: martinun242@gmail.com <martinun242@gmail.com>
Sent: 6/6/2019 11:34:22 AM
Subject: Your transaction 41279321 is on its way to Nigeria

Hi Kenneth,

Great news! Your bank transfer to Kenneth Ogudu is being processed and we'll let you both know when the money has arrived into their account.

Here's everything you need to know:

Your transaction number: 41279321
You sent: USD 276.99
Kenneth gets: NGN 95370.75
Bank name: ACCESS BANK
Bank account: 0765989561
When Kenneth should receive their money: Within minutes

Did you know you can track your transfer in our app on iOS and Android? Just go to your transaction history and tap on your transaction to follow your money along its journey.

And if you have any questions, head to our FAQ to find the answer.

Thanks again for using us!
WorldRemit Customer Service

From: Martin graham <martinun242@gmail.com>
To: customerservice@worldremit.com <customerservice@worldremit.com>
Sent: 7/25/2019 2:03:02 PM
Subject: Fwd: Bank statement and all information
Attachments: CFNetworkDownload_r6qBMe.tmp.list.pdf

My name is Kenneth Ogudu attached is my bank statement as requested for my pending transactions with transfer number (43378706). I am business man who's into (car sales)Secondly I am also the recipient of the money as it's been needed for my urgent use. Thanks in anticipation on your urgent response.

Warm Regards,
Kenneth Ogudu .

From: Kenneth Ogudu <kennethogudu52@gmail.com>
To: martinun242@gmail.com <martinun242@gmail.com>
Sent: 7/25/2019 1:54:32 PM
Subject: Fwd: Bank statement and all information
Attachments: CFNetworkDownload_r6qBMe.tmp.list.pdf

Sent from my iPhone

Begin forwarded message:

From: Kenneth Ogudu <kennethogudu52@gmail.com>
Date: 24 July 2019 at 11:35:21 AM GMT-4
To: customerservice@worldremit.com
Subject: Fwd: Bank statement and all information

Sent from my iPhone

My name is Kenneth Ogudu attached is my bank statement as requested for my pending transactions with transfer number (43378706). I am business man who's into (car sales)Secondly I am also the recipient of the money as it's been needed for my urgent use. Thanks in anticipation on your urgent response.

Warm Regards,
Kenneth Ogudu .

35. Investigators also discovered that a "Dan Moore" had emailed OGUDU after Victim J.J. knew Moore had supposedly died, asking for help to use various online dating profiles. These emails are posted below:

From: Dan moore <danmoore051@yahoo.com>
To: Martinun242@gmail.com <Martinun242@gmail.com>
Sent: 9/29/2019 1:46:06 PM
Subject: Update
Attachments: 40 (1).jpg; 43.jpg

Working name : Danny Moore
Age : 57
Eye : Blue
Relationship status : Widower

password : gingerboy

sign up email : danmoore6@protonmail.com

From: Dan moore <danmoore051@yahoo.com>
To: Martinun242@gmail.com <Martinun242@gmail.com>
Sent: 9/29/2019 1:49:33 PM
Subject: update

match
ourtime
eharmony

Help me open these profiles brother

Victim L.T.

36. Victim L.T., who resided in Missouri, met a woman online through the dating app, "Hinge" that he knew as Zainab Spencer ("Spencer").Victim L.T. and Spencer began to communicate frequently, usually through text messages, and soon the two began on online relationship. Spencer told Victim L.T. that she was in the military stationed away from the United States. Victim L.T. believed that he would marry Spencer upon her return to the United States.

37. Spencer told Victim L.T. she had a loan from the military that she needed help repaying. advised he had sent her $50,000.00 to help her pay back the loan. On another occasion, Spencer told Victim L.T. she had been involved in a car accident, where she had hit someone else, and asked for money to help with the costs. Other times, Spencer claimed her bank account was blocked and she needed money. Victim L.T. stated something would always pop up. Victim L.T. estimated he had sent Spencer approximately $100,000.00 over time. These transactions were through iTunes cards, where he would take a picture of the back of the card and then send to her. Victim L.T. stated he had purchased Bitcoin for Spencer on multiple occasions. He had utilized

Cash App and had also sent wire transfers. Spencer also asked Victim L.T. to send another woman $1,000.00 through PayPal.

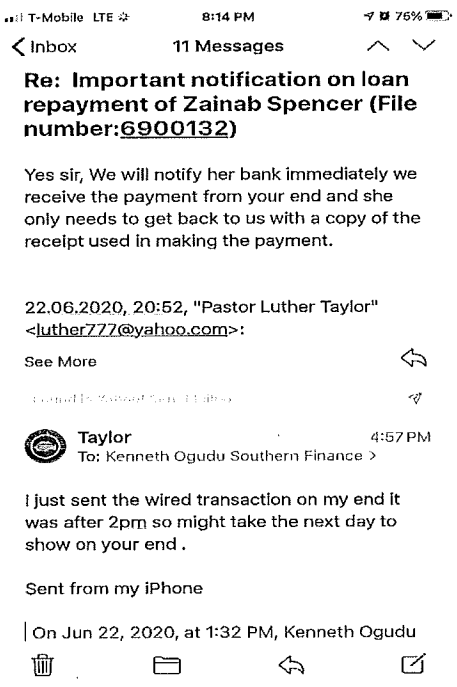
38. On one occasion, Spencer informed Victim L.T. that her supervisor had given her an opportunity to start a project making facemasks for the Covid-19 pandemic for the Army. Spencer told Victim L.T. she had not been provided any money for the project. Spencer estimated the project would cost between $50,000 to $70,000 and asked for Victim L.T. to send her the money. Victim L.T. stated he sent her the money little by little, and Spencer had promised to pay him back. Victim L.T. further advised these payments were sent to Spencer through Bitcoin and Cash App.

39. Victim L.T. was interviewed by investigators on November 27, 2020. Victim L.T. informed investigators that he last spoke with Spencer the weekend before this interview. Spencer informed Victim L.T. that her grandmother's account had been frozen and wanted Victim L.T. to link his credit card to her account. Victim L.T. advised he refused to give her the credit card information.

40. Victim L.T. wired $30,000.00 wire transfer to OGUDU on June 23, 2020. Victim L.T. advised he had sent the transfer, but he did not remember the purpose for the transfer or whether this specific transaction was related to the facemask project. OGUDU emailed Victim L.T. at least 8 times between June 22, 2020 and June 24, 2020.

41. According to records obtained through the investigation and information from cooperating witnesses, OGUDU was residing at the SUBJECT PREMISES when the $30,000 wire transfer was deposited into his account and these emails were sent to Victim L.T.

Examples of the emails from OGUDU



T-Mobile LTE 8:14 PM 76%

Inbox 11 Messages

Re: Important notification on loan repayment of Zainab Spencer (File number:6900132)

Yes sir, We will notify her bank immediately we receive the payment from your end and she only needs to get back to us with a copy of the receipt used in making the payment.

22.06.2020, 20:52, "Pastor Luther Taylor" <luther777@yahoo.com>:

See More

Taylor 4:57 PM
To: Kenneth Ogudu Southern Finance >

I just sent the wired transaction on my end it was after 2pm so might take the next day to show on your end .

Sent from my iPhone

On Jun 22, 2020, at 1:32 PM, Kenneth Ogudu

T-Mobile LTE 12:24 AM 74%

Inbox 19 Messages

Update my bank call me back today They di...

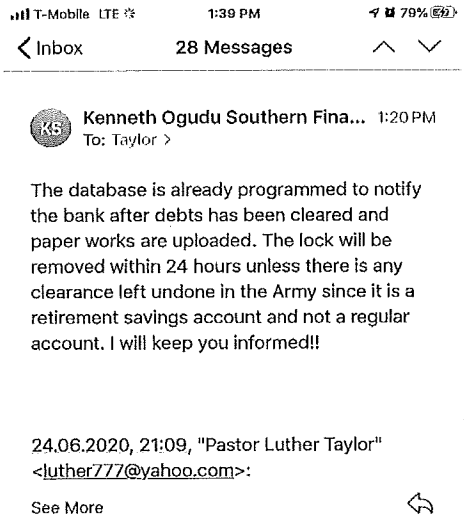
Kenneth Ogudu Southern Fi... Yesterday
To: Taylor >

Re: Important notification on loan repayment of Zainab Spencer (File number:6900132)

Okay sir, I will check with the bank tomorrow to check the status of the transaction, you can be rest assured since your bank confirmed it went through.

24.06.2020, 01:03, "Pastor Luther Taylor" <luther777@yahoo.com>:

See More



T-Mobile LTE 1:39 PM 79%

Inbox 28 Messages

Kenneth Ogudu Southern Fina... 1:20 PM
To: Taylor >

The database is already programmed to notify the bank after debts has been cleared and paper works are uploaded. The lock will be removed within 24 hours unless there is any clearance left undone in the Army since it is a retirement savings account and not a regular account. I will keep you informed!!

24.06.2020, 21:09, "Pastor Luther Taylor" <luther777@yahoo.com>:

See More

FINANCIAL ANALYSIS

42. At least from 2017 to the summer of 2020, NASSY, HARRISON, EMENI, OGUDU, THORPE, and AWOLESI operated fraud schemes and the information below summarizes the amount of proceeds each subject received from illegal activity. Investigators' review of EMENI, NASSY, HARRISON, OGUDU, THORPE, and AWOLESI's reported wages for the period from March 2017 through March 2020, revealed low wages for most of these individuals.

OGUDU

43. A review of OGUDU's known bank accounts shows that he received wires or other deposits from at least 12 different individuals currently believed to be fraud victims from May 30, 2019 until November 15, 2019, which total to approximately $253,448 at this time. However, as the financial breakdown below shows, OGUDU is believed to have received more fraud proceeds through cash deposits, deposits from co-conspirators, and transfers from other sources such as Money Gram, Western Union, Pay Pal and Zelle. OGUDU was born on October 29, 1992 and is 28 years old. OGUDU reported $400 in 2017 and 2018 and did not file taxes in 2019. Investigators have been unable to uncover any reported wages for OGUDU from the period March 2017 until March 2020.

Deposits Received from Victims	$253,448.00
Cash Deposits	$ 5,308.00
Deposits from Co-Conspirators	$ 7,920.00
Deposits from Pay Pal, Square, Cash App, Xoom, TransferWise, Zelle, Ping Express, Money Gram Western Union, and Walmart	$ 58,189.28
Total Illegal Proceeds Received by OGUDU	**$ 324,865.28**

Example of Victim Funds Deposited in OGUDU's Bank Account

CHASE

JPMorgan Chase Bank, N.A.
P O Box 182051
Columbus, OH 43218-2051

August 24, 2019 through September 25, 2019
Account Number: 000000503285907

CUSTOMER SERVICE INFORMATION

Web site:	Chase.com
Service Center:	1-800-935-9935
Deaf and Hard of Hearing:	1-800-242-7383
Para Espanol:	1-877-312-4273
International Calls:	1-713-262-1679

00027634 DRE 001 211 26919 NNNNNNNNNNN 1 000000000 17 0000
KENNETH OSEME OGUDU
2014 9TH AVE
HUNTINGTON WV 25703-1802

CHECKING SUMMARY Chase Total Checking

	AMOUNT
Beginning Balance	**$2,964.82**
Deposits and Additions	86,654.99
ATM & Debit Card Withdrawals	-35,554.11
Electronic Withdrawals	-25,887.49
Other Withdrawals	-8,000.00
Fees	-89.50
Ending Balance	**$20,088.71**

TRANSACTION DETAIL

DATE	DESCRIPTION	AMOUNT	BALANCE
	Beginning Balance		**$2,964.82**
08/26	Deposit 1043317270	100.00	3,064.82
08/26	Quickpay With Zelle Payment From Thao Hong Hoang 8573527053	2,000.00	5,064.82
08/26	Payment Sent 08/23 Code 28D988 Www.Remitly.C WA Card 0859	-920.99	4,143.83
08/26	Quickpay With Zelle Payment To Pnc Jpm26313761 8	-1,500.00	2,643.83
08/26	Quickpay With Zelle Payment To Anwulika Jpm26313771 1	-150.00	2,493.83
08/26	Payment Sent 08/24 Code F655F0 Www.Remitly.C WA Card 0859	-145.47	2,348.36
08/26	Card Purchase 08/24 5459 Dominos Pizza 865-675-3030 TN Card 0859	-29.46	2,318.90
08/26	Quickpay With Zelle Payment To Cy(Sls) Jpm263449416	-400.00	1,918.90
08/26	Quickpay With Zelle Payment To Kayode G Akanbi 8576865366	-100.00	1,818.90
08/27	Quickpay With Zelle Payment From Ablodun Afolabi 8581044680	250.00	2,068.90
08/27	Card Purchase 08/26 Ping Express Dallas TX Card 0859	-1,701.99	366.91
08/28	Card Purchase Return 08/27 Ping Express Dallas TX Card 0859	1,701.99	2,068.90
08/28	Fedwire Credit Via: Midsouth Bank, NA/065203431 B/O: Ruth Ann Brassfield Zwolle LA 71486-0000 Ref: Chase Nyc/Ctr/Bnf=Kenneth Oseme Ogudu Huntington, WV 257031802/Ac-0000 00005032 Rfb=O/B Midsouth Nat Obi=P Ersonal Loan Imad: 0828Mmqfmpag000023 Trn: 4887609240Ff	9,000.00	11,068.90
08/28	Fedwire Credit Via: First National Bank of Pennsylvania/043318092 B/O: Hong X Huynh West Reading PA 19611 Ref: Chase Nyc/Ctr/Bnf=Kenneth Oseme Ogudu Huntington, WV 257031802/Ac-0000 00005032 Rfb=O/B Fnb of PA Obi=Rest Aurant Appliance Purchase Imad: 0828L1Lfbu8C000466 Trn: 6052509240Ff	3,000.00	14,068.90

CHASE

August 24, 2019 through September 25, 2019
Account Number: 000000503285907

TRANSACTION DETAIL (continued)

DATE	DESCRIPTION	AMOUNT	BALANCE
08/28	Chips Credit Via: Wells Fargo Bank, N.A /0509 B/O: Jeffery Paulus Papua New Guinea Ref: Nbnf=Kenneth Oseme Ogudu Huntington, WV 257031802/Ac-000000005032 Org=/1006859753 Papua New Guinea Ogb=Ba Nk of South Pacific Ltd Port Moresb Y, Papau New Guinea Obi=School Fee Assistance Bbi=/Chgs/USD25,00/ Ssn: 0083451 Trn: 1715800240Fc	1,697.00	15,765.90
08/28	Quickpay With Zelle Payment From Thao Hong Hoang 8582255108	2,000.00	17,765.90
08/28	Quickpay With Zelle Payment From Harshit Verma 8583652391	100.00	17,865.90
08/28	Payment Sent 08/27 Code 3F7D12 Www.Remitly.C WA Card 0859	-253.99	17,611.91
08/28	ATM Withdrawal 08/28 1000 5th Ave Huntington WV Card 0859	-2,328.00	15,283.91
08/28	Domestic Incoming Wire Fee	-15.00	15,268.91
08/28	Domestic Incoming Wire Fee	-15.00	15,253.91
08/28	Domestic Incoming Wire Fee	-15.00	15,238.91
08/29	Payment Sent 08/28 Code Be7CA7 Www.Remitly.C WA Card 0859	-485.99	14,752.92
08/29	Transfer To Chk Xxxxxx9770	-5,000.00	9,752.92
08/29	ATM Withdrawal 08/29 1000 5th Ave Huntington WV Card 0859	-3,000.00	6,752.92
08/29	Card Purchase With Pin 08/29 Cvs/Pharmacy #04 04419 Huntington WV Card 0859	-86.16	6,666.76
08/29	Quickpay With Zelle Payment To Ebuka Jpm264723135	-300.00	6,366.76
08/30	Fedwire Credit Via: Midsouth Bank, NA/065203431 B/O: Ruth Ann Brassfield Zwolle LA 71486-0000 Ref: Chase Nyc/Ctr/Bnf=Kenneth Oseme Ogudu Huntington, WV 257031802/Ac-0000 00005032 Rfb=O/B Midsouth Nat Obi=P Ersonal Loan Imad: 0830Mmqfmpag000032 Trn: 7081609242Ff	3,000.00	9,366.76
08/30	Payment Sent 08/29 Code 1701Cb Www.Remitly.C WA Card 0859	-506.99	8,859.77
08/30	ATM Withdrawal 08/30 1000 5th Ave Huntington WV Card 0859	-2,480.00	6,379.77
08/30	Recurring Card Purchase 08/29 Google *Youtube Tv 855-836-3987 CA Card 0859	-49.99	6,329.78
08/30	Domestic Incoming Wire Fee	-15.00	6,314.78
09/03	Quickpay With Zelle Payment From Ablodun Afolabi 8607557608	75.00	6,389.78
09/03	ATM Withdrawal 08/31 1000 5th Ave Huntington WV Card 0859	-2,984.00	3,405.78
09/03	ATM Withdrawal 08/31 1000 5th Ave Huntington WV Card 0859	-360.00	3,045.78
09/03	Quickpay With Zelle Payment To Precious Smallie 8598338490	-20.00	3,025.78
09/03	Quickpay With Zelle Payment To Ebuka Jpm266023636	-250.00	2,775.78
09/03	Payment Sent 09/01 Code 96283D Www.Remitly.C WA Card 0859	-286.95	2,488.83
09/03	Quickpay With Zelle Payment To Anwulika Jpm266153567	-200.00	2,288.83
09/03	Card Purchase 09/02 Remitly 877-526-4216 WA Card 0859	-358.69	1,930.14
09/03	Quickpay With Zelle Payment To Cy(Sis) Jpm266545828	-1,500.00	430.14
09/03	Quickpay With Zelle Payment To Sreehari Sreenath 8607562117	-38.80	391.34
09/03	Quickpay With Zelle Payment To Benik Afobe 8607563496	-78.00	313.34
09/04	Quickpay With Zelle Payment From Thao Hong Hoang 8610117584	2,000.00	2,313.34
09/04	Quickpay With Zelle Payment From Ablodun Afolabi 8610283866	760.00	3,073.34
09/04	Payment Sent 09/03 Cash App*Kenneth Em 8774174551 CA Card 0859	-211.00	2,862.34
09/04	Quickpay With Zelle Payment To Kayode G Akanbi 8610281415	-1,500.00	1,362.34
09/05	Payment Sent 09/04 Code 653549 Www.Remitly.C WA Card 0859	-1,273.99	88.35
09/05	Recurring Card Purchase 09/05 Vesta *AT&T Prepaid 866-608-3007 OR Card 0859	-42.80	45.55

INFORMATION LEARNED FROM EMAIL SEARCH WARRANTS

44. Law enforcement previously applied for and received numerous email search warrants. Investigators received information from several email addresses victims contacted during the fraud scheme as well as the Targets' email addresses. In their review of the information from the email addresses, investigators learned that OGUDU used online banking and could access their bank information, including bank statements, deposit and transfer history electronically. Many of the Targets also used services such as Zelle and CashApp to transfer money between one another. Consequently, the Targets often had Zelle or CashApp transaction

records emailed to them. The emails also revealed that EMENI transferred money to one of OGUDU's foreign bank accounts. HARRISON similarly transferred money to one of NASSY's bank accounts held overseas.

Examples of transfers seen in EMENI's email account:

Sent: Fri, 15 Dec 2017 13:37:52 +0000
Subject: OLUWAGBENGA T HARRISON sent you $900.00
From: "Chase QuickPay Team" <no-reply@alertsp.chase.com>
Sent: Fri, 15 Dec 2017 13:37:52 +0000
To: emenikenneth5@gmail.com

OLUWAGBENGA T HARRISON sent you money through Chase QuickPay(R) with Zelle(SM), we're processing the payment. Your sender is registered with a Zelle member bank that suppo time payments. You'll usually get their payment in a few minutes.

Payment Details:
Amount: $900.00 (USD)
Memo:

Sent: Tue, 20 Mar 2018 13:09:07 +0000
Subject: JOHN R NASSY sent you $1,600.00
From: "Chase QuickPay Team" <no-reply@alertsp.chase.com>
Sent: Tue, 20 Mar 2018 13:09:07 +0000
To: emenikenneth5@gmail.com

JOHN R NASSY sent you money through Chase QuickPay(R) with Zelle(SM), and we're processing the payment. Your sender is registered with a Zelle member bank that supports real-time payments. You'll usually get their payment in a few minutes.

Payment Details:
Amount: $1,600.00 (USD)
Memo: Debt payment

Sent: Tue, 08 Oct 2019 16:27:46 +0000
Subject: You sent Kenneth Ogudu $1,180.00
From: Sendwave <sendwave@sendwave.com>
Sent: Tue, 8 Oct 2019 16:27:46 +0000
To: emenikenneth5@gmail.com

Hi Kenneth Emeni,

Your money transfer has arrived in Kenneth Ogudu's Access account! It may take up to 48 hours to appear in your statement.

Here's a receipt of the transaction for your records:

Sender: Kenneth Emeni
Recipient Name: Kenneth Ogudu
Recipient Number: •••9561
Amount Sent: 1180.00 USD
Amount Received*: 416540 NGN
Exchange Rate: 353.00 NGN/1 USD
Transaction Time: Oct 8, 2019, 4:27:20 PM EDT It may take up to 48 hours to appear in your statement.
Funds Available: Oct 8, 2019, 4:27:20 PM EDT
Confirmation Number: BAN-191008-PRP8B7

Email us at help@sendwave.com if you have any questions about this transaction!

45. OGUDU's email accounts had either screenshots or emails where each had forwarded their banking information to others in an apparent effort to further the fraud scheme. THORPE also forwarded his banking information to the martinun242@gmail.com account, which was linked to OGUDU as explained in Paragraphs 48-49 of the Affidavit.

Examples where OGUDU forwards his and others' banking information from this email address to the Martinun242@gmail.com account:

Name Kenneth Ogudu

Acc # 503285907

Routing #051900366

Bank address 1000 5th Ave, Huntington, WV 25701

Account Type : checking

Swift codeCHASUS33

Bank name J.P. Morgan chase bank

0765989561
Access

6264

Kennethogudu042
Capital098

Name: Thao Hong hoang
State : Florida
City : 7050 W 4th Ln Hialeah
ZipCode : 33014

Name : Thao Hong hoang

Routing:267084131
Acc 396967389

Bank Addy 401 W 49th st, Hialeah FL 33012

House addy
7050 W 4th Ln Hialeah

Name: Larry bellony Fernández

Bank: TD bank

Type: checking

Account. 4334175472

Routing: 031201360

Address: 9001 flatbush Brooklyn n.y 11236

Name. Francisco Guzmán

Bank. Santander

Type. Checking

Account. 9530838174

Routing. 231372691

Address. 1 unión square Elizabeth Nj 07201

From: Kenneth Ogudu <kennethogudu52@gmail.com>
To: Martinun242@gmail.com <Martinun242@gmail.com>
Sent: 3/31/2018 6:28:34 AM
Subject: Fwd: Acc

---------- Forwarded message ----------
From: **Kenneth Ogudu** <kennethogudu52@gmail.com>
Date: Friday, October 27, 2017
Subject: Acc
To: Mrlogin392@gmail.com

Account name VICKY PHONGSA
ACCOUNT NUMBER 196476010455
Routine number 073000545
Ssn 230-21-2869 my mother maiden name is prasasouk, my birthday is aug 3rd 1967
Addy 508 E.ECULID AVE. DES MOINES, IA
50313

Example when THORPE forwards his own banking information to the Martinun242@gmail.com account:

From: Thorpe, Romello <thorpe8@live.marshall.edu>
To: martinun242@gmail.com <martinun242@gmail.com>
Sent: 11/10/2019 3:57:49 PM
Subject: Romello Thorpe

c #002261206256
r #054001204 & 026009593
Bank of America
3500 georgia ave nw 20010

Get Outlook for iOS

46. OGUDU also forwarded the martinun242@gmail.com various documents he appeared to have created to further the online fraud schemes. For example, OGUDU or one of his co-conspirators forwarded one victim what investigators believe is a fake passport created to lull the victim into believing that she was corresponding with the person she thought was her romantic interest. Similarly, OGUDU or one of his co-conspirators also forwarded another victim a travel itinerary which appears to be created by OGUDU or one of his co-conspirators in furtherance of the fraud as well.

Example One:

Sent: Sat, 31 Mar 2018 06:27:44 +0000
Subject: Passport
From: "Kenneth Ogudu" <kennethogudu52@gmail.com>
Sent: Sat, 31 Mar 2018 06:27:44 +0000
To: "Martinun242@gmail.com" <Martinun242@gmail.com>
4828EB6B-83A5-4151-AC1C-F97436BB6946.jpeg

Example Two:

From: Kenneth Ogudu <kennethogudu52@gmail.com>
To: martinun242@gmail.com <martinun242@gmail.com>
Sent: 6/11/2019 3:29:33 PM
Subject: Fwd: MARTIN/PHAM 24JUN2019 IAH MIA
Attachments: Itinerary.pdf; STAR_ITIH0_ITI_1064894_1.png; STAR_ITIH0_ITI_1064894_1.png

Sent from my iPhone

Begin forwarded message:

From: "MADERISE TRAVELS AND TOURS" <maderisetravels@gmail.com>
Date: 11 June 2019 at 10:01:47 AM GMT-4
To: KENNETHOGUDU52@GMAIL.COM
Subject: MARTIN/PHAM 24JUN2019 IAH MIA

Your trip

Booking ref: KV9W6N Check My Trip
Document Issue Date: 11 June 2019

Traveler Pham Martin

Agency MADERISE TRAVELS AND TOURS
52, Allen Avenue, Ikeja
LAGOS
Telephone +2348098945400
Email maderisetravels@gmail.com

Monday 24 June 2019

From: Martin graham <martinun242@gmail.com>
To: Thao Hoang <Thaoh89@gmail.com>
Sent: 6/11/2019 3:31:32 PM
Subject: : MARTIN/PHAM 24JUN2019 IAH MIA
Attachments: Itinerary.pdf; STAR_ITIH0_ITI_1064894_1.png; STAR_ITIH0_ITI_1064894_1.png

Your trip

Booking ref: **KV9W6N** Check My Trip
Document Issue Date: **11 June 2019**

Traveler **Pham Martin**

Agency MADERISE TRAVELS AND TOURS
52, Allen Avenue, Ikeja
LAGOS
Telephone +2348098945400
Email maderisetravels@gmail.com

Monday 24 June 2019

47. The martinun242@gmail.com account also had several emails from services such as Hushed or TextNow letting the email user know that their assigned number was expiring. Hushed is an online app which allows users to have a second phone number. Users can use this second phone number to make calls, send text and picture messages all while keeping their primary number private. Textnow is a service that assigns a free phone number to the app user. A review of the data collected from the email search warrants also revealed that one of the email accounts that a victim had communicated during the fraud scheme had various documents which discussed "How to Set Up a Fake Bank Account."

AFFIANT BACKGROUND IN FINANCIAL CRIMES INVESTIGATIONS

48. As a Special Agent with the Secret Service, your Affiant has had training and experience in financial crimes investigations. Based upon my training, experience, and knowledge, I am aware of the following:

a. Monetary instruments, such as checkbooks, money orders, and cashier's

checks, utilized by individuals engaged in illegal activities such as financial fraud schemes are oftentimes secured in safe-deposits, locked drawers, and lock boxes.

b. In these types of online fraud schemes, victims often mail packages to the perpetrators of the fraud. The packages can have cash, various gift cards and even iphones, laptop computers or watches inside.

c. Individuals involved in other illegal activities oftentimes place income and assets in the name of nominees, in hopes of shifting the responsibility for the payment of tax and concealing their ownership to protect the assets from seizure. However, it is also my experience that the titles and deeds to said assets are maintained by the subject and not the nominee owner.

d. Analysis of business and personal financial records created and maintained by legal and illegal business entities can determine the validity of the books and records and provide leads to the expenditure of illegal or wrongfully obtained proceeds.

e. Business entities generally require that specific business and personal financial records be maintained for use in applying for loans at financial institutions, for tax preparation, and for audit purposes. These records are commonly stored for lengthy periods of time at residences, at business offices, in vehicles and other storage facilities.

f. Records can be stored in paper format or in digital form. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small

devices that are plugged into a port on the computer - can store thousands of documents. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person and can store digital copies of records. Smartphones and other smart electronic devices also often have access to online banking accounts through mobile applications or web browsers. These accounts are often utilized to maintain the business records of expenses and income.

g. The Internet affords individuals several different venues for obtaining, completing, and storing business records.

i. Individuals also use online resources to retrieve and store records. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of records may be found on the user's computer, smartphone, or external media in some cases.

ii. A digital technology related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or

playing a game – on a mobile device. Individuals commonly use such apps to engage in banking activity, money transfers, bill payments, and engage in other financial related activities.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for purposes of maintaining records. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

i. Paper copies, or hard copies, of business and personal financial records can also be stored in file cabinets, desk drawers, cabinets, safes and safe-deposit boxes, lock boxes, wallets, purses and handbags, garbage bags, cardboard boxes, and other storage containers large enough for paper retention.

j. Individuals engaged in conspiracies to commit other crimes often communicate with one another as well as with unwitting accomplices. These communications can occur in many forms including person to person, telephonic, text messages and electronic such as email. These communications typically involve details pertaining to the scheme, directions to subordinates as

to how to carry out certain elements of the scheme and correspondence to and from unwitting third parties such as financial institutions, investors, and accountants.

k. Individuals involved in criminal endeavors conduct financial transactions in a manner to avoid law enforcement detection. These individuals exchange currency for various types of monetary instruments including postal money orders, cryptocurrencies, and bank cashiers' checks and, thereby, attempt to disguise and conceal their true business and personal affairs.

l. To accurately reconstruct the personal and business financial histories of persons and their various businesses, all forms of business and personal records reflective of financial transactions are required.

49. Your Affiant has no reason to believe that the search is likely to result in the seizure of any drafts of publications (such as books, newsletters, website postings, etc.) that are unrelated to the search and stored on the target computers. Thus, the search will not implicate the Privacy Protection Act, 42 U.S.C. § 2000aa. I have no reason to believe that the search is likely to result in the seizure of a mail server. Thus, the search will not implicate the Electronic Communications Privacy Act, 18 U.S.C. § 2701.

50. Your Affiant believes that given the continuing nature of financial crimes, as well as the length of the scheme, there is probable cause to believe that evidence of violations of federal law, including, but not limited to, 18 U.S.C. § 1341 (mail fraud); 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1956 (laundering in monetary transactions in property derived from specified unlawful activity); and 18 U.S.C. § 1957 (engaging in monetary transactions in property derived from specified unlawful activity), will be present in the SUBJECT PREMISES as described in

Attachment B, and on the person of OGUDU as described in Attachment A, when the search is conducted. Thus, even if OGUDU uses an electronic device (such as a laptop or a mobile smart phone) to access the Internet and digital records, his own financial records, there is probable cause that evidence of this access will be found in the SUBJECT PREMISES in addition to being on each of their individual persons and devices seized.

BACKGROUND ON SEIZURE AND SEARCH PROCEDURES FOR ELECTRONIC DEVICES AND DIGITAL EVIDENCE IN RELATION TO FRAUD INVESTIGATIONS

51. As described further in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B), of any device belonging to or used OGUDU or where ownership cannot be determined.

52. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. As detailed in the Victim Information Section above, various perpetrators of the fraud scheme used cellphones, computers, and other electronic devices to communicate with the victims during the fraud scheme. Electronic devices were critical to carrying out this fraud scheme. The emails within the martinun242@gmail.com account show that the fraudsters used digital devices to help create various lulling documents to further the fraud. Similarly, several of the victims were defrauded by Bitcoin scams, by either sending money to purchase Bitcoin or opening up Bitcoin wallets on behalf of the fraudsters. As

Bitcoin is a cryptocurrency, it is held virtually. Similarly, evidence of fraudulent Bitcoin transfers would also most likely be digital evidence.

b. The information gathered from the email search warrants shows that EMENI, NASSY, HARRISON, OGUDU, THORPE and AWOELSI used electronic devices to carry out these frauds, whether by making financial transfers or sending banking information to their other co-conspirators.

c. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

e. Wholly apart from user-generated files, computer storage media, in particular, computers' internal hard drives, contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few

examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

f. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

53. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer

file systems can record information about when the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of

computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Lastly, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an

accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. I know that when an individual uses a computer to complete illegal financial activities, the individual's computer will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of a crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

54. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either

seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

55. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime — including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

56. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might

expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. The process by which the search and seizure of such computers or other electronic devices will occur in this instance is more formally laid out in Attachment B.

BIOMETRIC ACCESS TO DEVICES

57. This warrant permits law enforcement to compel OGUDU to unlock any electronic devices ("DEVICES") or computers requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follow:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different

names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric

passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for eight hours *and* the passcode or password has not been entered in the last six days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a

locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of OGUDU to the fingerprint scanner of the DEVICES found at the PREMISES; (2) hold the DEVICES found at the PREMISES in front of the face of OGUDU and activate the facial recognition feature; and/or (3) hold the DEVICES found at the PREMISES in front of the face of each of OGUDU and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel OGUDU state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel OGUDU to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

PROBABLE CAUSE SUMMARY

58. Based on the victim interviews and financial records, there is probable cause to believe that each of the Targets is involved in a fraud scheme which regularly used email, text messaging and other electronic and Internet based methods of communication as well as money transfers. As stated earlier in the Affidavit, each of the Targets has been charged by a federal Grand

Jury on fraud charges in 3:21-cr-00068. Specifically, EMENI and HARRISON each face multiple charges alleging violations of 18 U.S.C. § 1343 (wire fraud) as well as a violation of 18 U.S.C. § 1957 (unlawful monetary transaction) and 18 U.S.C. § 2315 (receipt of stolen property). NASSY is facing multiple charges alleging violations of 18 U.S.C. § 1341 (mail fraud), as well 18 U.S.C. § 1343 and 18 U.S.C. § 2315 violations. AWOLESI faces charges alleging violations of 18 U.S.C. § 1343 and 18 U.S.C. § 2315. OGUDU and THORPE are each facing charges alleging violations of 18 U.S.C. § 1343, 18 U.S.C. § 2315 and a violation of 18 U.S.C. § 1956 (conspiracy to commit money laundering.)

CONCLUSION

59. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

60. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

REQUEST FOR SEALING

It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search

warrant. Your Affiant believes that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation. Premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

TERRY HEDRICK
SPECIAL AGENT
UNITED STATES SECRET SERVICE

Subscribed and sworn-to by the Affiant telephonically in accordance with the procedures of Rule 4.1 of the Federal Rules of Criminal Procedure, on May 25, 2021.

CHELSEY A. VASCURA
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF OHIO